EXHIBIT A-1

General Terms and Conditions

1 **Safeguards.** In addition to the controls specified in the exhibits to this Agreement, External Party agrees to implement administrative, physical, and technical safeguards to protect the availability, confidentiality and integrity of Metropolitan Government of Nashville and Davison County (Metro Government) Information, information technology assets and services.. All such safeguards shall be in accordance with industry-wide best security practices and commensurate with the importance of the information being protected, but in no event less protective than those safeguards that External Party uses to protect its own information or data of similar importance, or is required by applicable federal or state law.

2 **Inventory.** External Party agrees to maintain at all times during the Term of this Agreement a Product and Service Inventory. External Party shall upon request of Metro Government, which shall be no more frequently than semi-annually, provide the current Product and Service Inventory to Metro Government within thirty (30) days of the request.

3 **Confidentiality.**

3.1 **General.** External Party and its Agents shall access, use and disclose Metro Government Information only when it is necessary to perform External Party's obligations as required under the Purchasing Agreement or this Agreement. Additionally, External Party shall not use, authorize to use or disclose Metro Government Information for the purpose of developing information or statistical compilations for use by third parties or other division or subsidiary of External Party or for any commercial exploitation, unless otherwise agreed upon in writing by Metro Government. External Party and its Agents shall maintain the confidentiality of any Metro Government Information and shall not disclose it other than to persons in its organization who have a need to know and who are bound by a duty of confidentiality no less protective to the Metro Government Information than this section.

3.2 **Return/Destruction of** Metro Government Information**.** Upon the termination of an applicable Purchasing Agreement or upon Metro Government's request, External Party shall (i) immediately cease to access and use the Metro Government Information per Metro Government's request, or, if due to termination of a Purchase Agreement, cease to access and use the Metro Government Information received pursuant to or otherwise relating to the terminated Purchasing Agreement, (ii) return to Metro Government, or destroy, such Sensitive Information and all copies thereof within ten (10) days of the termination or request, and (iii) upon Metro Government's request, certify in writing to Metro Government that it has complied with its obligations set forth in this section. To the extent that any Metro Government Information is contained in Archived Data and return or destruction of the same according to this section is unduly burdensome, External Party shall destroy such Metro Government Information in accordance with External Party's general data destruction policies, but in no event shall External Party retain the Archived Data or Metro Government Information for a time period exceeding what is required under applicable law. If no such time period exists under the applicable law, then External Party shall not retain archived Metro Government Information for more than one (1) year from Metro Government's request for destruction or return or otherwise the termination of the applicable Purchasing Agreement.

4 **Data Ownership.** As between Metro Government and External Party, all Metro Government Information are the exclusive property of Metro Government. In no event shall External Party claim any rights with respect to such Metro Government Information or take any action with respect to such Metro Government Information that is inconsistent with the duties of a bailee for hire under applicable law. External Party hereby waives any and all statutory and common law liens it may now or hereafter have with respect to Metro Government Information. Nothing in this Agreement, Purchasing Agreement or any other agreement between the Metro Government and External Party shall operate as an obstacle to Metro Government's right to retrieve any and all Metro Government Information from External Party or its Agents or to place such data with a third party or Metro Government for provision of service to Metro Government, including, without limitation, any outstanding payments, overdue payments and/or disputes, pending legal action or arbitration. Upon Metro Government's request, External Party shall supply Metro Government with an inventory of Metro Government Information that External Party Stores and/or backed up.

5 **Connection of Systems or Devices to the Metro Government Network.** External Party shall not place any systems or devices on the Metro Government Network without the prior written permission of the Director of ITS, designee, or the designated Metro Government contact for this Agreement.

6 **Access Removal.** If granted access to Metro Government Network or systems, External Party and its Agents shall only access those systems, applications or data which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent External Party or its Agent from accessing those data or functions outside of Metro Government's authorization. External Party shall impose reasonable sanctions against any Agent who attempts to bypass security controls. Notwithstanding anything to the contrary in the Purchasing Agreement or other agreement between Metro Government and External Party, Metro Government at its sole discretion, may refuse granting access right to Metro Government Network or Sensitive Information to any Agent of External Party, and may at any time remove access rights (whether physical premise access or system access) from External Party or any Agents, without prior notice or liability to External Party, if Metro Government reasonably suspects a security violation by External Party or such Agent or otherwise deems such action appropriate to protect Metro Government Infrastructure, Metro Government Network or Metro Government Information.

7 **Virus Representation and Warranty.** External Party represents and warrants that Products and Services, or any media upon which the Products are stored, do not have, nor shall External Party or its Agents otherwise introduce into Metro Government's systems, Metro Government Network or Metro Government Infrastructure, any type of software routines or element which is designed to or capable of unauthorized access to or intrusion upon, disabling, deactivating, deleting or otherwise damaging or interfering with any system, equipment, software, data, or the Metro Government Network. In the event of a breach of this representation and warranty, External Party shall compensate Metro Government for any and all harm, injury, damages, costs, and expenses incurred by Metro Government resulting from the breach.

8 **Subcontracting/Outsourcing.**

8.1 **Prior Approval.** Without Metro Government's prior written consent, External Party may not subcontract with a third party to perform any of its obligations to Metro Government which involves access to Metro Government Information or connection to Metro Government Network. Nor shall External Party outsource any External Party infrastructure (physical or virtual) which Stores Sensitive Information without such consent. To obtain Metro Government's consent, External Party shall complete and sign the form attached as Exhibit A-4 and send it to Metro Government's Information Security /Incidents/Data Breach contact listed in Exhibit A-3. In addition, Metro Government may withdraw any prior consent if Metro Government reasonably suspect a violation by the subcontractor or outsource provider of this Agreement, or otherwise deems such withdraw necessary or appropriate to protect Metro Government Network, Metro Government Infrastructure or Metro Government Information.

8.2 **Agent Confidentiality.** External Party Agents are bound by the same confidentiality obligations set forth in this Agreement. External Party or its Agent may not transfer, provide access to or otherwise make available Metro Government Information to any individual or entity outside of the United States (even within its own organization) without the prior written consent of Metro Government. To obtain such consent, External Party shall send Metro Government a notice detailing the type of information to be disclosed, the purpose of the disclosure, the recipient's identification and location, and other information required by Metro Government.

8.3 **External Party Responsibility.** Prior to subcontracting or outsourcing any External Party's obligations to Metro Government, External Party shall enter into a binding agreement with its subcontractor or outsource service provider ("Third Party Agreement") which (a) prohibits such third party to further subcontract any of its obligations, (b) contains provisions no less protective to Metro Government Network, Metro Government Infrastructure and/or Metro Government Information than those in this Agreement, and (c) expressly provides Metro Government the right to audit such subcontractor or outsource service provider to the same extent that Metro Government may audit External Party under this Agreement. External Party warrants that the Third Party Agreement will be enforceable by Metro Government in the U.S. against the subcontractor or outsource provider (e.g., as an intended third party beneficiary under the Third Party Agreement). Without limiting any other rights of Metro Government in this Agreement, External Party remains fully responsible and liable for the acts or omissions of its Agents. In the event of an unauthorized disclosure or use of Sensitive Information by its Agent, External Party shall, at its own expense, provide assistance and cooperate fully with Metro Government to mitigate the damages to Metro Government and prevent further use or disclosure.

9 **Indemnity.**

9.1 **Indemnification.** Notwithstanding any disclaimer and/or limitation of liability contained in a Purchasing Agreement and in addition to any indemnity obligation set forth in a Purchasing Agreement, External Party shall defend, indemnify and hold harmless Metro Government and their respective successors, assigns, directors, officers, agents and employees (collectively, "Indemnitees") from and against any and all liabilities, demands, losses, consequential damages, penalties, costs to mitigate, expenses, fines, amounts paid in settlements or judgments, and all other reasonable expenses and costs incident thereto including, without limitation, court costs and reasonable attorneys' fees (collectively, "Damages") arising out of or resulting from any claim, lawsuit, demand, investigation, proceeding, regulatory action, or other cause of action directly or indirectly relating to the breach or alleged breach by External Party or its Agents of any representations, warranties, obligations, terms, or covenants contained in this Agreement (collectively, "Action").

9.2 **Indemnification Process.** If any Action is commenced against an Indemnitee, written notice shall be provided to External Party, External Party shall undertake the defense of such Action and the Indemnitee shall reasonably cooperate with External Party in the defense to whatever reasonable extent External Party requires and at External Party's sole expense. External Party shall have the right to settle or compromise such Action at External Party's expense for the benefit of the Indemnitee; provided, however, the Indemnitee may not be obligated in any respect in connection with such compromise or settlement without the its prior written consent. Notwithstanding the foregoing, if External Party fails to assume its obligation to defend, the Indemnitee may do so to protect its interest and seek reimbursement from External Party.

10 Audit.

10.1Internal Review and Audit Report. Upon Metro Government's request, External Party shall provide a copy of the report on controls within External Party's organization and systems under Statement on Standards for Attestation Engagements (SSAE) No. 16, or under standards established by an authorized or recognized standard setting organization (such as the International Auditing and Assurance Standards Board). Such review and report will be conducted at External Party's operations center at External Party's cost by an independent auditing firm for the purposes of verifying the safety and soundness of the Products and/or Services.

10.2Compliance Audit. Metro Government shall have the right, at its expense, during normal business hours and with reasonable advance notice, to evaluate, test, and review at External Party's premises or via the use of remote assessment tools, the Products and Services to ensure compliance with the terms and conditions of this Agreement. Metro Government shall have the right to conduct such audit by use of its own employees and internal audit staff, or by use of outside consultants and auditors. In conducting such audit, Metro Government shall have the right to execute copies of software Products on External Party's computer systems, at no cost to Metro Government. External Party shall cooperate with and provide reasonable assistance to Metro Government and provide all pertinent books and records (including, but not limited to, system and facility maintenance records, Product and Service vulnerability reports, relevant Audit Log files and External Party's internal information security assessment report) and other information reasonably requested by Metro Government in connection with such audit at no additional cost to Metro Government.

10.3Confidentiality. External Party is not obligated to divulge any trade secrets or proprietary information of External Party or any third party except to the extent necessary to satisfy the purpose of the audit contemplated by this section. In no event shall External Party be obligated to divulge any trade secrets or proprietary information to any of its direct competitors or the affiliate of such competitor. Metro Government agrees that with respect to any External Party Sensitive information received in connection with such audit, Metro Government, its employees, and its outside consultants and auditors shall be subject to the same confidentiality obligations as set forth in Section 3.1 above to the extent applicable.

11 Miscellaneous.

11.1Term; Survival. The Term of this Agreement commences on the Effective Date and shall remain in effect until the later of the termination of all Purchasing Agreement(s) or when all Metro Governments cease to use any Products purchased, licensed, leased, rented or otherwise acquired from External Party or receive any Services from External Party. Sections 3, 4, 5, 9, 11 and those terms which by their nature are intended to survive the expiration of this Agreement shall so survive.

11.2Governing Law; Venue; Severability; Attorneys' Fees. The validity, interpretation, and performance of this Agreement shall be controlled and governed by the laws of the State of Tennessee, without regard to conflicts of law provisions.

Jurisdiction and venue for any dispute between External Party and any Metro Government concerning this Agreement shall exclusively rest within the State and Federal Courts of Davidson County, Tennessee. In the event of any litigation between External Party and Metro Government related to this Agreement, and in the event Metro Government prevails in that litigation, Metro Government shall be awarded all costs, expenses, and legal fees (including reasonable attorneys' fees) it incurred in connection with such litigation. If any provision of this Agreement or the application of any such provision is held by a court of competent jurisdiction to be contrary to law, the remaining provisions of this Agreement shall continue in full force and effect.

11.3<u>Injunctive Relief; Litigation Assistance</u>. External Party acknowledges that monetary remedies may be inadequate to protect Metro Government's rights hereunder and that, in addition to legal remedies otherwise available, injunctive relief is an appropriate remedy to protect such rights. External Party agrees to provide assistance and cooperation upon the reasonable request of Metro Government in connection with any action against third parties to protect the Sensitive Information.

11.4<u>Remedy Under Purchasing Agreement.</u> A material breach of this Agreement by External Party and/or its Agents shall be deemed a material breach under the relevant Purchasing Agreement(s), with the rights and remedies of the parties under such agreements being applicable to any such breach. Further, in the event External Party fails to remedy any material breach of this Agreement within fifteen (15) days of receipt of written notice from Metro Government describing the nature of the alleged breach, Metro Government may elect to terminate and be relieved of any future purchasing or payment obligations under the Purchasing Agreement(s).

11.5<u>Conflicts.</u> For avoidance of doubt, this Agreement is independent of and is not subject or subordinate to any Purchasing Agreement or any other agreement between the parties. In the event of a conflict between this Agreement, the relevant Purchasing Agreement, and/or the Business Associate Agreement, the provision(s) that provides more protection, grants more right or otherwise is more favorable to Metro Government shall control. This Agreement shall replace and supersede all prior Information Security Agreement(s) that may have been entered into between External Party and Metro Government or its Affiliate for the same Product and/or Service. If there is any ambiguity or conflict between the terms within this Agreement (including all exhibits), the provision or interpretation that provides Metro Government and/or Metro Government Information or Sensitive Information stronger protection shall control.

11.6<u>Waiver, Integration, Amendment.</u> The failure by either party to exercise any right provided hereunder shall not be deemed a waiver of such right. Any ambiguity in this Agreement shall not be interpreted against either party and shall be interpreted as if each party hereto had prepared this Agreement. This Agreement and the provisions in the relevant Purchasing Agreements and any Business Associate Agreement(s) addressing the subject matter hereof constitute the entire understanding and agreement between the parties with respect to the subject matter hereof, and supersedes all prior and contemporaneous agreements, understandings, negotiations and discussions, whether oral or written, of the parties and/or subsidiaries of the parties. This Agreement may be amended, modified, or supplemented only by writing signed by the parties to this Agreement and which expressly states intent to so amend this Agreement. The titles and the italicized descriptions in the exhibits are for convenience only and shall not be used to interpret any provision of this Agreement.

11.7<u>Successors and Assigns</u>. Neither party may assign, transfer or subcontract any rights or obligations under this Agreement in whole or part without the prior written consent of the other party. Any assignment, transfer or subcontract without such consent shall be deemed void and of no effect. Such consent shall not be unreasonably withheld nor shall compensation be required. However, either party may assign, without written consent, this Agreement and its rights and obligations to any successor entity resulting from a merger or consolidation of such party or, in the case of Metro Government, to any entity controlled by, controlling or under common control with Metro Government. Subject to the foregoing, all of the terms, conditions, covenants, and agreements contained herein shall inure to the benefit of, and be binding upon, any such successor entity or permitted assignees of the respective parties hereto, with the parties hereto being responsible for the obligations and liabilities of their respective successors, assignees, or transferees. It is further understood and agreed that consent by either party to such assignment in one instance shall not constitute consent by the party to any other assignment.

EXHIBIT A-2

Definitions

Capitalized terms used in the Agreement shall have the meanings set forth in this Exhibit A-2. Terms not defined in this Exhibit A-2 or otherwise in the Agreement shall have standard industry meanings.

1. “Affiliates” as applied to any particular entity, means those entities, businesses, and facilities that are controlled by, controlling, or under common control with a stated entity, as well as (with respect to Metro Government) any entity to which Metro Government and/or any of the foregoing provides data processing services.

2. “Agent” means any subcontractor, independent contractor, officer, director, employee, consultant or other representative of External Party, whether under oral or written agreement, whether an individual or entity.

3. “Agreement” means this Information Security Agreement, including all applicable exhibits, addendums, and attachments.

4. “Antivirus Signatures” means a catalog of data that describes the current Malicious Software threats (e.g., virus, worms, spyware) and how Antivirus Software is to detect and remove the threat from the given system, message or file.

5. “Antivirus Software” means an A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.

6. “Archived Data” means information that is retained solely for backup or archival purposes in accordance with External Party’s backup policies.

7. “ASP” means “Application Service Provider”.

8. “Audit Log” means a chronological record of system activities. Includes records of system accesses and operations performed in a given period.

9. “Authentication Credentials” means information that is used to verify the identity of a user, process or device and is a prerequisite to allowing access to other information. Includes but not limited to: passwords, SecurID PINs, and encryption keys (excluding public certificates)**.**

10. “Backdoor Software” means any code, function or software that allows a user to bypass normal authentication and/or authorization functions or other security controls to a product and/or system, which would allow the user to remain undetected or un-audited.

11. “Cardholder Data” means data as defined by the Payment Card Industry (PCI) Security Standard Council, which is the full magnetic stripe, or the Primary Account Number (PAN) plus any of the following: (a) Cardholder name, (b) Expiration date, or (c) Service Code (Capitalized terms in this definition have the meanings set forth in the PCI Data Security Standard)

12. “Certify General Compatibility” means a commercially reasonable process or means to test that a Product will still operate without diminishing its functionality or speed of processing data and all functions are still available and functioning properly after some change to the Product or to its dependent third party product, such as after a Security Patch has taken place.

13. “Critical Security Patch” means a Security Patch that mitigates or remedies a Critical Vulnerability.

14. “Critical Vulnerability” means any Vulnerability that would allow an individual or system without access rights or proper credentials to gain administrative-like access to a Product or Service or to data contained therein or whose exploitation could allow code execution without user interaction.. For example, a compromise that would allow authorized unfettered or administrative-like access, include without limitation, administrative access to the Product or Service, full access or control of a data store, and/or the ability to alter Audit Logs. Determination of “Critical” is determined by the vendor’s assessment of the vulnerability or of a Common Vulnerability Scoring System base score of “high”.

15. “Data Breach” means any actual or suspected unauthorized disclosure or use of, or access to, Metro Government Information, or actual or suspected loss of Metro Government Information.

16. “Disaster Recovery Plan” means a written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

17. “Effective Date” means the date first set forth on page 1 of the Agreement.

18. “Electronic Protected Health Information” or “EPHI” means PHI as defined in 45 C.F.R. 160.103 of the HIPAA regulations in electronic form.

19. “Encrypt” or “Encrypted” means the process of transforming information (referred to as plaintext) using an algorithm (cipher) to make the information unreadable except to those possessing special knowledge, usually referred to as a key.

20. “HIPAA” means the Health Insurance Portability and Accountability Act of 1996, as amended, and the regulations related thereto.

21. “IAAS” means “Infrastructure As A Service.”

22. “Important Security Patch” means a Security Patch that mitigates or remedies an Important Vulnerability.

23. “Important Vulnerability” means a Vulnerability in the Product or Service that would allow a user who already had access to the Product or Service to obtain unauthorized access rights or compromise the Product or Service in some way or whose exploitation could result in compromise of the confidentiality, integrity, or availability of user data, or of the integrity or availability of processing resources. Determination of “Important” is determined by the vendor’s assessment of the vulnerability or of a Common Vulnerability Scoring System base score of “medium”.

24. “Information Security Incident” means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

25. “Interactive User Login” means the process by which a person, as opposed to a system or application, manually identifies and authenticates himself as a user of a system or device (for example, by typing in a username and password).

26. “Metro Government Information” means an instance of an information type belonging to Metro Government. Any communication or representation of knowledge, such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual, owned by or entrusted to Metro Government.

27. “Metro Government Infrastructure” means any information technology system, virtual or physical, which is owned, controlled, leased, or rented by Metro Government, either residing on or outside of the Metro Government Network. Metro Government Infrastructure includes infrastructure obtained from an IAAS provider or systems that are provided and located on the Metro Government Network as part of a Service.

28. “Metro Government Network” means any Wide Area Network (WAN) or Local Area Network (LAN) owned, operated, managed or controlled by Metro Government.

29. “Malicious Software” is defined as a program that is written intentionally to carry out annoying or harmful actions, which includes Trojan horses, viruses, and worms.

30. “NIST” means the National Institute of Standards and Technology.

31. “Off-the-Shelf Software” or “OTS” means an item that is (1) sold, leased, or licensed to the general public; (2) offered by a External Party trying to profit from it; (3) supported and developed by the External Party who retains the underlying intellectual property rights; (4) available in multiple, identical copies; and (5) used without modification of the internal code.

32. “Open Network” means any open, unsecured or untrusted network such as the Internet.

33. “Open Source Software” means software that is licensed pursuant to the provisions of any "open source" license agreement including, without limitation, any version of any software licensed pursuant to any GNU General Public License (GNU GPL) or GNU Lesser/Library Public License (LGPL), or Mozilla Public License (MPL), or any other license agreement that requires source code be distributed or made available in connection with the distribution of the licensed software in object code form or that limits the amount of fees that may be charged in connection with sublicensing or distributing such licensed software**.**

34. “Principle of Least Privilege” is the principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

35. “Product” means any software, hardware, system, computer equipment or product provided by External Party to Metro Government.

36. **“**Product and Services Assumptions” shall have the meaning set forth in Section 3 of the Agreement.

37. “Product and Service Inventory” means a complete, accurate and current inventory of all Products and Services provided by External Party to Metro Government.

38. “Protected Health Information” or “PHI” shall have the meaning set forth at 45 C.F.R. 160.103 of the HIPAA regulations.

39. “Purchasing Agreement” means any agreement between External Party and any Metro Government for the purchase, lease, licensing, acquisition or servicing of a Product or provision of Services, regardless whether Metro Government has any payment obligations under the agreement.

40. “Remote Access” means access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet).

41. “Remote Access Software” means any technology that can provide Remote Access to the Metro Government Network.

42. “Remote Control Software” means any program or application which uses Remote Access to connect to a machine, system or application and control, manage or administer such machine, system or application.

43. “Responsible Disclosure” means disclosure of a Vulnerability to the External Party by a third party where the Vulnerability is kept secret for an agreed upon time so that External Party can create, test, document and release a Security Patch to address the Vulnerability.

44. “Risk Management” means the process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system, and includes: 1) the conduct of a risk assessment; 2) the implementation of a risk mitigation strategy; and 3) employment of techniques and procedures for the continuous monitoring of the security state of the information system.

45. “SaaS” means “software as a service” or “software on demand”.

46. “Security Patch” means a patch, bug fix, software update, upgrade, new release, new version, modification, improvement, enhancement or fix designed to repair known problems in previous software releases in order to prevent unauthorized access, destruction, or corruption of data, or exploitation of a Vulnerability.

47. “Sensitive Information” – Any information classified as "Confidential" or "Restrictive" as defined by the *Metropolitan Government Information Classification Policy*.

48. “Service(s)” means any service provided by External Party (or its Agents) to Metro Government, including but not limited to, maintenance and support service, program development service, consulting service, outsourcing service, or other professional service.

49. “Session Timeout” means a security control or function that automatically logs a user off and ends the current use session of the Product after a defined period of inactivity.

50. “Store” means the act of backing up, saving, keeping, recording or otherwise writing or storing any data or information in any type of permanent media or permanent storage device. For the avoidance of doubt, this excludes temporarily storing information to a dynamic and volatile RAM.

51. "Strong Authentication" means an authentication system that leverages two different types of data that serve as proof of the identity of the specific user trying to authenticate (e.g., a certificate and a password, a password and the answer to a secret user question, SecurID Token Code and PIN, or a password and encrypted session cookie). User Identifiers (UIDs) are never considered one of the factors in Strong Authentication.

52. "Strong Encryption" or "Strongly Encrypted" means an Encryption algorithm that meets industry standard criteria, as defined by NIST. Whenever External Parties are required to use Strong Encryption the cryptographic modules used must be validated to Federal Information Processing Standards (FIPS)140-1 Security Requirements for Cryptographic Modules, and other FIPS cryptography based standards.

53. "Strong Hash Algorithm" means a hash value that is commercially resistant to forgery. The strength of the hash algorithm is an industry standard as defined by NIST.

54. "Term" means the period during which this Agreement is in effect.

55. "External Party Managed System" means (i) any system, device or application which is owned, leased or rented by Metro Government or its Affiliates, which is managed or administered by External Party on behalf of Metro Government or its Affiliates, and (ii) any External Party-owned systems which reside on the Metro Government Network and managed or administered by External Party.

56. "Vulnerability" means a flaw or weakness in a Product's or system's security procedures, design or implementation that could be exercised (accidentally triggered or intentionally exploited) and result in harm or unauthorized access to a system, activity or Metro Government Information.

EXHIBIT A-3

Communication and Contacts

All communications relating to this Agreement will be directed to those contact persons specified herein. To the extent External Party has different contact persons for different Products and/or Services, such contact persons should be listed in this exhibit or an attachment to this exhibit. External Party shall promptly notify Metro Government of any changes to these contact persons. All notices required under this Agreement shall be in writing (which includes email or facsimile) and shall be deemed to have been given when the designated person(s) of the receiving party actually receives such notice. Email notice is preferred.

The principal and alternative contact persons for **day-to-day compliance** with this Agreement are:

		Principal Contact	Alternate Contact
Metro Government:	Name:	Jeff Gossage	DEPARTMENT HEAD
	Title:		
	Phone:		
	Email:		
	Address:		

□ For all Products/Services

If different contacts for different Products/Services, list contact information by each Product and/or Service.

		Principal Contact	Alternate Contact
External Party:	Name:		
	Title:		
	Phone:		
	Email:		
	Address:		

The contact persons for **Information Security/Incidents/Data Breach** are:

		Principal Contact	Alternate Contact
Metro Government:	Name:	John Griffey	ITS Help Desk
	Title:		
	Phone:		
	Email:		
	Address:		

		Principal Contact	Alternate Contact
External Party:	Name:		
	Title:		
	Phone:		
	Email:		
	Address:		

The contact persons for receiving **legal notice** under this Agreement and for escalation of any compliance issues related to this Agreement are:

		Principal Contact	Alternate Contact
Metro Government:	Name:	Jeff Gossage	Theresa Costonis
	Title:		
	Phone:		
	Email:		
	Fax:		
	Address:		

		Principal Contact	Alternate Contact
External Party:	Name:		
	Title:		
	Phone:		
	Email:		
	Fax:		
	Address:		

EXHIBIT A-4

Subcontractor Disclosure and Approval

Prior to External Party subcontracting or outsourcing any Services or IT infrastructure (physical or virtual), External Party shall complete this form and obtain Metro Government's written approval.

External Party Questions	External Party Responses
What Products or Services is the subcontracting/outsourcing related to?	
What functions or External Party obligations are to be performed by the subcontractor/outsource provider?	
What is the identity and legal name of the subcontractor/outsource provider?	
What is the physical address of the subcontractor/outsource provider?	
Where will the infrastructure be physically located, if External Party will outsource its infrastructure?	
Where will the subcontractor perform the Services or obligations owed by External Party to Metro Government?	
What kind of network connection, and to what systems/application, will the subcontractor/outsourced infrastructure require?	
What Metro Government data or information will be disclosed, transmitted or stored by the subcontractor/outsource provider or its agents (please specify whether disclose, transmit or store)?	
Does the subcontractor/outsource provider have the right to further subcontract/outsource the functions relevant to Metro Government?	
Does Metro Government have the right to audit such subcontract/outsource provider's system and records to the same extent External Party allows Metro Government under this Agreement?	

External Party agrees to notify Metro Government immediately upon its knowledge of any change to the information provided above, which in External Party's reasonable and responsible judgment, may expose Metro Government's networks, Metro Government Infrastructure, and/or Metro Government Information to greater risk than before the change took place. Metro Government may withhold and revoke its consent to External Party subcontracting or outsourcing any Service or obligation at its sole discretion and at any time without liability to External Party or any third party.

By signing below, External Party represents and warrants that the information provided above is and will remain accurate and complete (to the extent controllable by External Party) during the Term of this Agreement.

By signing below, Metro Government grants its consent to External Party subcontracting or outsourcing the Service/obligation described above, provided that if any of the information above changes after the date herein, Metro Government may revoke such consent.

Metropolitan Government of Nashville and Davidson County		External Party	
Name:	Metropolitan Government of Nashville and Davidson County	Name:	
By:		By:	
Name:		Name:	
Title:		Title:	
Date:		Date:	

<u>**EXHIBIT ACSA**</u>

Any Agent who requires access to Metro Government Network shall sign the following agreement, which shall be collected and maintained by such Metro Government, before being granted access to any system or data.

Agent Confidentiality and Security Agreement

Capitalized terms not defined herein are defined in the relevant Information Security Agreement between Metro Government and the External Party.

1 General Agent Requirements.

1.1 I understand that I should have no expectation of privacy when using Metro Government's information systems. The Metro Government may log, access, review, and otherwise utilize information stored on or passing through its systems, including email, in order to manage systems and enforce security.

1.2 I understand that violation of this agreement may result in disciplinary action, up to and including loss of privileges, and/or termination of authorization to work within the Metro Government facility or with Metro Government Information.

2 Protecting Metro Government Information.

2.1 I will not disclose or discuss any Metro Government Information with others, including friends or family, who do not have a need to know it. I will not take media or documents containing Metro Government Information home with me unless specifically authorized to do so as part of my job.

2.2 I will not publish or disclose any Metro Government Information to others using personal email, or to any Internet sites, or through Internet blogs or sites such as Facebook or Twitter. I will only use such communication methods when explicitly authorized to do so in support of Metro Government Company business and within the permitted uses of Metro Government Information as governed by regulations such as HIPAA.

2.3 I will not in any way divulge, copy, release, sell, loan, alter, or destroy any Metro Government Information except as properly authorized. I will only reuse or destroy media in accordance with Metro Government's information security standards and Metro Government record retention policy (provided by Metro Government upon request).

2.4 I will not make any unauthorized transmissions, inquiries, modifications, or purging of Metro Government Information.

2.5 I will not transmit Metro Government Information outside the Metro Government's internal network unless I am specifically authorized to do so as part of my job responsibilities. If I do transmit Metro Government Information outside of the Company using email or other electronic communication methods, I will ensure that the data is encrypted according to Metro Government's information security standards, which the Metro Government will provide to Agent upon request.

2.6 I will not copy or store Metro Government Information on removable media or portable devices such as laptops, tablets, personal digital assistants (PDAs), cell phones, smartphones, CDs, thumb drives, external hard drives, etc., unless specifically required to do so by my job. If I do copy or store data on removable media or portable devices, I will encrypt the data while it is on the media according to Metro Government's information security standards, which the Metro Government will provide to Agent upon request.

3 Abiding by Appropriate Security Controls.

3.1 I will only access or use Systems or devices I am officially authorized to access, and will not demonstrate the operation or function of Systems or devices to unauthorized individuals.

3.2 I will not attempt to bypass Metro Government security controls.

3.3 I understand that I will be assigned a unique identifier to track my access and use of Metro Government Information and that the identifier is associated with my personal data provided as part of the initial and/or periodic credentialing and/or employment verification processes.

3.4 I will:

3.4.1 Use only my officially assigned User-ID and password (and/or token (*e.g.*, SecurID card)).

3.4.2 Use only licensed software.

3.5 I will never:

3.5.1 Disclose passwords, PINs, or access codes.

3.5.2 Use tools or techniques to break/exploit security measures.

3.5.3 Connect unauthorized Systems or devices to the Company network.

3.6 I will practice good workstation security measures such as locking my computer when away from my desk, using screen savers with activated passwords, positioning screens away from public view.

3.7 I will immediately notify the Metro Government Chief Information Security Officer or ITS Help Desk if:

3.7.1 my password has been seen, disclosed, or otherwise compromised;

3.7.2 media with Sensitive Information stored on it has been lost or stolen;

3.7.3 I suspect a virus infection on any System;

3.7.4 I am aware of any activity that violates this agreement, privacy and security policies; or

3.7.5 I am aware of any other incident that could possibly have any adverse impact on Metro Government Information or Metro Government Systems.

4 Upon Termination.

4.1 I agree that my obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the External Party.

4.2 Upon termination, I will immediately return any documents or media containing Metro Government Sensitive Information to the External Party.

4.3 Upon termination, I will immediately delete any Metro Government Information stored on devices not owned by the External Party or Metro Government and will be prepared to show proof of deletion.

4.4 I understand that I have no right to any ownership interest in any Metro Government Information accessed or created by me during and in the scope of my relationship with the Metro Government.

Agent Signature / External Party Name:		Date:	
Agent and External Party Printed Name:			
Business Entity Name:			

EXHIBIT AST

Agent Security and Training

1 **Background Check.** External Party shall perform a background check which includes a criminal record check on all Agents, who may have access to Metro Government Information. External Party shall not allow any Agents to access Metro Government Information or perform Services under a Purchasing Agreement if External Party knows or reasonably should know that such Agent has been convicted of any felony or has been terminated from employment by any employer or contractor for theft, identity theft, misappropriation of property, or any other similar illegal acts.

2 **Information Security Officer.** If Agents will access or handle Metro Government Information, External Party shall designate an Information Security Officer, who will be responsible for External Party information security and compliance with the terms of this Agreement as it relates to Metro Government Information.

3 **Agent Access Control.** External Party shall implement and maintain procedures to ensure that any Agent who accesses Metro Government Information has appropriate clearance, authorization, and supervision. These procedures must include:

3.1 Documented authorization and approval for access to applications or data stores which contain Metro Government Information; e.g., email from a supervisor approving individual access (note: approver should not also have technical rights to grant access to Sensitive Information); documented role-based access model; and any equivalent process which retains documentation of access approval.

3.2 Periodic (no less than annually) reviews of Agent user access rights in all applications or data stores which contain Sensitive Information. These reviews must ensure that access for all users is up-to-date, appropriate and approved.

3.3 Termination procedures which ensure that Agent's user accounts are promptly deactivated from applications or data stores which contain Sensitive Information when users are terminated or transferred. These procedures must ensure that accounts are deactivated or deleted no more than 14 business days after voluntary termination, and 24 hours after for cause terminations.

3.4 Procedures which ensure that Agent's user accounts in applications or data stores which contain Sensitive Information are disabled after a defined period of inactivity, no greater than every 180 days.

3.5 Procedures which ensure that all Agents use unique authentication credentials which are associated with the Agent's identity (for tracking and auditing purposes) when accessing systems which contain Sensitive Information.

3.6 External Party will maintain record of all Agents who have been granted access to Metro Government Sensitive Information. External Party agrees to maintain such records for the length of the agreement plus 3 years after end of agreement. Upon request, External Party will supply Metro Government with the names and login IDs of all Agents who had or have access to Metro Government Information.

4 **Agent Training.**

4.1 External Party shall ensure that any Agent who access applications or data stores which contain Metro Government Information are adequately trained on the appropriate use and protection of the data or information and the security of the application. Completion of this training must be documented and must occur before Agent may access any Sensitive Information. This training must include, at a minimum:

4.1.1 Appropriate identification and handling of Metro Government Information

4.1.1.1 Awareness of confidentiality requirements contained in this Agreement;

4.1.1.2 Procedures for encrypting Metro Government Information before emailing or transmitting over an Open Network, if the data classification of the information requires these controls;

4.1.1.3 Procedures for data storage on media or mobile devices (and encrypting when necessary).

4.1.2 Education about the procedures for recognizing and reporting potential Information Security Incidents;

4.1.3 Education about password maintenance and security (including instructions not to share passwords);

4.1.4 Education about identifying security events (e.g., phishing, social engineering, suspicious login attempts and failures);

4.1.5 Education about workstation and portable device protection; and

4.1.6 Awareness of sanctions for failing to comply with External Party security policies and procedures regarding Sensitive Information.

4.1.7 Periodic reminders to Agents about the training topics set forth in this section.

4.2 External Party shall ensure that any Agent who accesses applications or data stores which contain Metro Government Information are adequately trained on the appropriate use and protection of this information. Completion of this training must be documented and must occur before Agent may access any Metro Government Information. This training must include, at a minimum:

4.2.1 Instructions on how to identify Metro Government Information.

4.2.2 Instructions not to discuss or disclose any Sensitive Information to others, including friends or family.

4.2.3 Instructions not to take media or documents containing Sensitive Information home unless specifically authorized by Metro Government to do so.

4.2.4 Instructions not to publish, disclose, or send Metro Government Information using personal email, or to any Internet sites, or through Internet blogs such as Facebook or Twitter.

4.2.5 Instructions not to store Metro Government Information on any personal media such as cell phones, thumb drives, laptops, personal digital assistants (PDAs), unless specifically authorized by Metro Government to do so as part of the Agent's job.

4.2.6 Instructions on how to properly dispose of Metro Government Information, or media containing Metro Government Information, according to the terms in Exhibit DMH as well as applicable law or regulations.

5 **Agent Sanctions.** External Party agrees to develop and enforce a documented sanctions policy for Agents who inappropriately and/or in violation of External Party's policies and this Agreement, access, use or maintain applications or data stores which contain Sensitive Information. These sanctions must be applied consistently and commensurate to the severity of the violation, regardless of level within management, and including termination from employment or of contract with External Party.

EXHIBIT AV

Protection Against Malicious Software

1 **Microsoft Systems on Metro Government Networks.** For Products which will be installed on Microsoft Windows Systems residing on Metro Government Network, External Party warrants that the Product will operate in conjunction with Metropolitan Government Antivirus Software, and will use real time protection features.

2 **Non-Microsoft Systems on Metro Government Networks.** For Products installed on non-Microsoft Windows Systems residing on Metro Government Network, External Party shall allow Metro Government to install Antivirus Software on such Products where technically possible. Upon Metro Government's request, External Party shall provide the requisite information to implement such Antivirus Software in a manner which will not materially impact the functionality or speed of the Product.

3 **All External Party Managed Systems.** For External Party Managed Systems, External Party shall install and maintain ICSA Labs certified or AV-Test approved Antivirus Software and, to the extent possible, use real time protection features. External Party shall maintain the Anti-virus Software in accordance with the Antivirus Software External Party's recommended practices. In addition, External Party shall ensure that: (i) the Antivirus Software checks for new Antivirus Signatures no less than once per day and (ii) the related Antivirus Signatures are current and no less recent than two versions/releases behind the most current version/release of the Antivirus Signatures for the Antivirus Software.

EXHIBIT BU

Data Backup

1 **General.**

1.1 External Party agrees to backup Metro Government Information which External Party maintains or Stores. Backup and restoration procedures and related infrastructure, including frequency of backup, offsite storage, media lifespan and media reliability, must be commensurate with the criticality and availability requirement of the Metro Government Information being backed up.

1.2 Upon Metro Government's request, External Party shall supply Metro Government with an inventory of Metro Government Information that External Party Stores and/or backed up.

1.3 External Party shall periodically, no less often than annually, test backup tapes or media by restoring Metro Government Information to a system similar to the original system where the Metro Government Information are stored.

1.4 Upon Metro Government's request, External Party shall supply copies of Metro Government Information in a format requested by Metro Government.

1.5 External Party shall backup business critical information at a frequency determined by Metro Government business owner.

2 **Storage of Backup Media.** External Party shall store archival and backup media in a secured offsite location. Upon request, External Party will promptly notify Metro Government of the physical address of the offsite location. The backups of the data should be stored in a manner commiserate with the security around the data. The backup tapes should be encrypted if the sensitivity of the data requires that level of security.

EXHIBIT CP

Contingency Plan

1 **Disaster Recovery Plan.** External Party will maintain a Disaster Recovery Plan for all applications or data stores which contain business critical information. This plan will outline the procedures necessary to restore business critical information on the application or systems in a timely fashion in the case of an emergency or disaster.

2 **Emergency Mode Operation Plan.** External Party shall maintain an emergency mode operating plan which ensures that systems or applications using or accessing business critical information are operational during an emergency or natural disaster, or are made operational after a disaster in a prompt manner, commensurate with the criticality of the data on the system.

3 **Testing and Revision Procedure.** External Party agrees to test, at least annually, External Party Disaster Recovery Plan and emergency mode operations plan and maintain a documented procedure for such testing. External Party shall document the results and findings from such testing and revise the plan accordingly.

4 **Other Terms. If any additional terms apply, please insert below:**

- TBD

EXHIBIT DMH

Device and Storage Media Handling

1 **Portable Media Controls.** External Party (including its Agents) shall only store Metro Government Information on portable device or media when expressly authorized by Metro Government to do so. When External Party stores Metro Government Sensitive Information or on portable device or media, External Party shall employ the following safeguards:

1.1 Access to the device or media shall require a password or authentication;

1.2 The device or media shall be encrypted using Strong Encryption;

1.3 The workstation or portable device or media containing Metro Government Information must be clearly identified or labeled in such a way that it can be distinguished from other media or device which is not used to store Sensitive Information.

1.4 The device or media must be accounted for by a system or process which tracks the movements of all devices or media which contain Metro Government Information**.**

2 **Media Disposal.**

2.1 External Party shall only dispose of media containing Metro Government Information when authorized by Metro Government.

2.2 External Party shall dispose of any media which stores Metro Government Information in accordance with media sanitization guidelines for media destruction as described in NIST document NIST SP800-88: Guidelines for Media Sanitization. The Guidelines are currently available at http://csrc.nist.gov/publications/PubsSPs.html

2.3 Upon Metro Government request, External Party shall promptly provide written certification that media has been properly destroyed in accordance with this Agreement.

2.4 External Party may not transport or ship media containing Metro Government Information unless the media is Encrypted using Strong Encryption, or the data on the media has been sanitized through complete data overwrite (at least three passes); or media destruction through shredding, pulverizing, or drilling holes (e.g. breaking the hard drive platters).

3 **Media Re-Use.**

3.1 External Party shall not donate, sell, or reallocate any media which stores Metro Government Information to any third party, unless explicitly authorized by Metro Government**.**

3.2 External Party shall sanitize media which stores Metro Government Information before reuse by External Party within the External Party facility.

EXHIBIT ENC

Encryption and Transmission of Data

1 External Party shall Encrypt Metro Government Sensitive Information whenever transmitted over the Internet or any untrusted network using Strong Encryption. Encryption of Sensitive Information within the Metro Government Network, or within External Party's physically secured, private data center network, is optional but recommended.

2 External Party shall Encrypt Metro Government Authentication Credentials while at rest or during transmission using Strong Encryption.

3 External Party shall Encrypt, using Strong Encryption, all Sensitive Information that is stored in a location which is accessible from Open Networks.

4 If data files are to be exchanged with External Party, External Party shall support exchanging files in at least one of the Strongly Encrypted file formats, e.g., Encrypted ZIP File or PGP/GPG Encrypted File.

5 All other forms of Encryption and secure hashing must be approved by Metro Government.

EXHIBIT IR

Incident Response

1 **Incident Reporting.** External Party shall report any Information Security Incident of which it becomes aware, or failure of any technical or procedural controls, which has or had a potential to affect Metro Government Network, Metro Government Infrastructure or Metro Government Information to the Information Security Incident contact listed in Exhibit A-3 and according to the following timeline and procedure:

1.1 External Party shall promptly report to Metro Government any successful Information Security Incident (with or without actual harm to system or data) within 24 hours of becoming aware of the incident. At a minimum, such report shall contain: (a) date and time when the Information Security Incident occurred; (b) the date and time when such incident was discovered by External Party; (b) identification of the systems, programs, networks and/or Metro Government Information affected by such incident; (c) preliminary impact analysis; (d) description and the scope of the incident; and (e) any mitigation steps taken by External Party However, if External Party is experiencing or has experienced a Data Breach or a successful Information Security Incident to systems that host or Store Sensitive Information or an Information Security Incident that is causing or has caused material disruption to the functionality or operation of External Party systems or damage to External Party hardware, software or data, including a successful attack by Malicious Software, External Party shall report such breach or incident to Metro Government both to the ITS Help Desk at (615) 862-HELP and the Information Security Incident contact listed in Exhibit A-3 within 24 hours from External Party's reasonable awareness of such breach or incident. For detailed requirement of Data Breach notification, see Exhibit RM.

1.2 External Party shall document any attempted but unsuccessful Information Security Incident of which it becomes aware and report to Metro Government upon its request. The frequency, content, and format of such report will be mutually agreed upon by the parties.

2 **Incident Response.**

2.1 External Party shall have a documented procedure for promptly responding to an Information Security Incidents and Data Breach that complies with applicable law and shall follow such procedure in case of an incident. External Party shall have clear roles defined and communicated within its organization for effective internal incidence response.

2.2 External Party shall designate a contact person for Metro Government to contact in the event of an Information Security Incident (such contact should be listed in Exhibit A-3). This contact person should possess the requisite authority and knowledge to: (i) act as a liaison to communicate between External Party and Metro Government regarding the incident (including providing information requested by Metro Government); (ii) perform the reporting obligations of External Party under this exhibit; and (iii) develop a mitigation strategy to remedy or mitigate any damage to Metro Government Network, Metro Government Infrastructure, Metro Government Information or the Product or Service provided to Metro Government that may result from the Information Security Incident.

EXHIBIT LOG

Audit Logs

1 **Audit Log Information**. The Product or Service will provide user activity Audit Log information. Audit Log entries must be generated for the following general classifications of events: login/logout (success and failure); failed attempts to access system resources (files, directories, databases, services, etc.); system configuration changes; security profile changes (permission changes, security group membership); changes to user privileges; actions that require administrative authority (running privileged commands, running commands as another user, starting or stopping services, etc.); and remote control sessions (session established, login, logout, end session, etc.). Each Audit Log entry must include the following information about the logged event: date and time of event; type of event; event description; user associated with event; and network identifiers (IP address, MAC Address, etc.) or logical identifiers (system name, port, etc.).

2 **Audit Log Integrity.** External Party shall implement and maintain controls to protect the confidentiality, availability and integrity of Audit Logs.

3 **User Access Audit.** Upon Metro Government's request, External Party shall provide Audit Logs of Metro Government's users of the Product or Service to Metro Government.

4 **Audit Log Feed.** Upon request, External Party shall implement a regular, but in no event less than daily, automated Audit Log feed via a secured, persistent connection to Metro Government Network so that Metro Government may monitor or archive Audit Log data relating to Metro Government's users on Metro Government systems.

5 **Audit Log Availability.**

5.1 External Party shall ensure that Audit Logs for the Product or Service for the past 90 days are readily accessible online.

5.2 If for technical reasons or due to an Information Security Incident, the online Audit Logs are not accessible by Metro Government or no longer trustworthy for any reason, External Party shall provide to Metro Government trusted Audit Log data for the past 90 days within 2 business days from Metro Government's request.

5.3 External Party shall provide or otherwise make available to Metro Government Audit Log data which are 91 days or older within 14 days from Metro Government's request.

5.4 External Party shall make all archived Audit Logs available to Metro Government no later than thirty (30) days from Metro Government's request and retrievable by Metro Government for at least one (1) year from such request.

5.5 External Party shall agree to make all Audit Logs available in an agreed upon format.

EXHIBIT NET

Network Security

1 Network Equipment Installation

1.1 External Party shall not install new networking equipment on Metro Government Network without prior written permission by the Metro Government **Information Security/Incidents/Data Breach** contact listed in Exhibit A-3. External Party shall not make functional changes to existing network equipment without prior written consent of such contact person for Metro Government.

1.2 External Party shall provide the Metro Government Information Security/Incidents/Data Breach contact listed in Exhibit A-3 with documentation and a diagram of any new networking equipment installations or existing networking equipment changes within 14 days of the new installation or change.

1.3 External Party shall not implement a wireless network on any Metro Government site without the prior written approval of the Metro Government Information Security/Incidents/Data Breach contact listed in Exhibit A-3, even if the wireless network does not connect to the Metro Government Network. Metro Government may limit or dictate standards for all wireless networking used within Metro Government facility or site.

2 **Network Bridging.** External Party shall ensure that no system implemented or managed by External Party on the Metro Government Network will bridge or route network traffic.

3 **Change Management.** External Party shall maintain records of External Party installations of, or changes to, any system on the Metro Government Network. The record should include date and time of change or installation (start and end), who made the change, nature of change and any impact that the change had or may have to the Metro Government Network, Metro Government system or Metro Government Information.

4 **System / Data Access.**

4.1 External Party and its Agents shall only access system, application or data which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent External Party or its Agent from accessing those data or functions outside of Metro Government's authorization. External Party shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.

4.2 External Party shall only use Metro Government approved methods to configure Metro Government systems or application or grant access to systems.

4.3 External Party shall use the Principle of Least Privilege when granting access to Metro Government Information, network or systems.

<u>**EXHIBIT PAT**</u>

Patch Creation and Certification

1 **<u>Security Patch Required</u>.** Unless otherwise expressly agreed by Metro Government and External Party, for Products that are no longer under performance warranty, External Party shall provide no less than standard maintenance and support service for the Products, which service includes providing Security Patches for the Products, for as long as Metro Government is using the Products.

2 **<u>Timeframe for Release</u>.** For Vulnerabilities contained within the Product that are discovered by External Party itself or through Responsible Disclosure, External Party shall promptly create and release a Security Patch. External Party must release a Security Patch: (i) within 90 days for Critical Vulnerabilities, (ii) within 180 days for Important Vulnerabilities, and (iii) within one (1) year for all other Vulnerabilities after External Party becomes aware of the Vulnerabilities. For Vulnerabilities contained within the Product that have become publicly known to exist and are exploitable, External Party will release a Security Patch in a faster timeframe based on the risk created by the Vulnerability, which timeframe should be no longer than thirty (30) days. For the avoidance of doubt, External Party is not responsible for creation of Security Patches for Vulnerabilities in the Product that is caused solely by the Off-the-Shelf Software installed by Metro Government.

3 **<u>Timeframe for Compatibility Certification</u>.** External Party shall promptly Certify General Compatibility of a Security Patch for third party software which the Product is dependent upon when such patch is released. For a Security Patch for Microsoft Windows Operating Systems, External Party shall Certify General Compatibility of a Critical Security Patch within five (5) days, and shall Certify General Compatibility of an Important Security Patch within thirty (30) days, from the release of the patch. For Security Patches for Off-the-Shelf Software (OTS), External Party shall Certify General Compatibility of a Critical Security Patch within five (5) days and Certify General Compatibility of an Important Security Patch within thirty (30) days from its release. For Security Patch for all other third party software or system, External Party shall Certify General Compatibility of a Critical Security Patch within five (5) days and an Important Security Patch within thirty (30) days from its release. . External Party shall publish whether the Security Patches are generally compatible with each related Product.

4 **<u>Notice of Un-patchable Vulnerability.</u>** If External Party cannot create a Security Patch for a Vulnerability, or Certify General Compatibility of a Security Patch for OTS software, within the timeframe specified herein, External Party shall notify Metro Government of the un-patchable Vulnerability in writing. Such notice shall include sufficient technical information for Metro Government to evaluate the need for and the extent of immediate action to be taken to minimize the potential effect of the Vulnerability until a Security Patch or any other proposed fix or mitigation is received.

5 **<u>Vulnerability Report.</u>** External Party shall maintain a Vulnerability Report for all Products and Services and shall make such report available to Metro Government upon request, provided that Metro Government shall use no less than reasonable care to protect such report from unauthorized disclosure. The Vulnerability Report should (a) identify and track all known Vulnerabilities in the Products or Services on a continuing and regular basis, (b) document all Vulnerabilities that are addressed in any change made to the Product or Service, including without limitation Security Patches, upgrades, service packs, updates, new versions, and new releases of the Product or Service, (c) reference the specific Vulnerability and the corresponding change made to the Product or Service to remedy the risk, (d) specify the critical level of the Vulnerability and the applicable Security Patch, and (e) other technical information sufficient for Metro Government to evaluate the need for and the extent of its own precautionary or protective action. External Party shall not hide or provide un-documented Security Patches in any type of change to their Product or Service.

6 **<u>SCCM Compatibility for Windows Based Products</u>.** External Party Patches for Products that operate on the Microsoft Windows Operating System must be deployable with Microsoft's System Center Configuration Manager.

EXHIBIT PES

Physical and Environmental Security

External Party shall implement security measures at any External Party facilities where Sensitive Information is stored. Such security measures must include, at a minimum:

1 Contingency Operations. A documented Disaster Recovery Plan for accessing the facility and the Sensitive Information, and restoring Sensitive Information if needed, in the case of an emergency or crisis.

2 Environmental Safeguards. Reasonable environmental safeguards to protect systems storing Sensitive Information from smoke, heat, water, fire, humidity, or power surge damage.

3 Access Control. Appropriate controls which ensure that only authorized personnel are allowed physical access to the facility. Examples of appropriate controls include, but are not limited to: signage; personnel badges and controlled badge access; visitor sign in, escort, and sign out; security guards; and video surveillance for data centers which store Sensitive Information.

4 Maintenance Records. External Party shall conduct regular maintenance on systems which contain Sensitive Information and to facility's physical and environmental controls (e.g., temperature, physical access). External Party shall maintain documentation of any repairs or maintenance performed on the systems or facility and shall provide Metro Government a copy of such records upon its reasonable request.

5 Physical Safeguards. External Party shall use best efforts to prevent theft or damage to External Party systems or storage media containing Sensitive Information. Such efforts shall include, but are not limited to:

5.1 Protecting systems or devices that contain un-encrypted Sensitive Information with physical barriers such as locked cabinet, floor to ceiling room, or secured cage.

5.2 Not storing Un-encrypted Sensitive Information in "multi-party" shared physical environments with other entities.

5.3 Not transporting or shipping un-encrypted media which stores Sensitive Information unless the data is sanitized through full media overwrite (at least one complete pass), or media destruction through shredding, pulverizing, or drive-punching (e.g., breaking the hard drive platters).

5.4 In the event Products generate, store, transmit or process Sensitive Information and the Product does not support encryption, External Party shall be solely responsible for the provision of physical security measures for the applicable Products (e.g., cable locks on laptops).

EXHIBIT PVPN

Perpetual and Special Network Connectivity

1 B2B VPN or Private Circuit Requirements.

1.1 For External Party's Business to Business (“B2B”) or private circuit network connections which terminate on the outside of the Metro Government Network, External Party must protect such connections by an ICSA Labs certified firewall.

1.2 Government may deny any traffic type due to risk and require External Party to use a more secured protocol. Microsoft protocols such as those used in Window File Shares are considered risky and will not be allowed.

1.3 B2B Virtual Private Network (“VPN”) connections to the Metro Government Network will only terminate on Metro Government managed network infrastructure.

1.4 External Party shall authenticate the VPN to the Metro Government Network using at least a sixteen (16) character pre-shared key that is unique to the Metro Government.

1.5 External Party shall secure the VPN connection using Strong Encryption.

1.6 External Party shall connect to the Metro Government Network using a device capable of Site-to-Site IPSec support.

1.7 External Party shall connect to the Metro Government Network using a device capable of performing policy-based Network Address Translation (NAT).

1.8 External Party shall connect to the Metro Government Network through the Metro Government VPN concentrator.

1.9 External Party shall not implement any form of private circuit access to the Metro Government network without prior written approval from the Metro Government Contact listed in Exhibit A-3.

1.10 Metro Government reserves the right to install filtering or firewall devices between External Party system and the Metro Government Network.

2 Requirements for Dial-In Modems.

2.1 If External Party is using an analog line, the analog line shall remain disconnected from the modem when not in use, unless Metro Government has expressly authorized permanent connection.

2.2 External Party shall provide the name of the individual(s) connecting to Metro Government Network and the purpose of the connection when requesting connectivity.

3 **System / Data Access.** External Party and its Agents shall only access system, application or data which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent External Party or its Agent from accessing those data or functions outside of Metro Government’s authorization. External Party shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.

EXHIBIT REM

Remote Access to Metro Government Network/System

1 Account Usage.

1.1 Upon request, External Party shall provide Metro Government with a list of active Agent user accounts and access levels and other information sufficient for Metro Government to deactivate or disable system access if it deems appropriate.

1.2 External Party may not share Metro Government-issued ID's, or any user accounts which grant access to Metro Government Network or Metro Government systems.

1.3 External Party Agent shall use unique accounts assigned to the Agent to perform work. Service accounts (or accounts that are configured and used by systems to gain access to information or other systems) may not be used by External Party Agents to access any system.

2 Metro Government Network Access Requirements.

2.1 External Party shall only use External Party systems which are compatible with Metro Government Remote Access technology to access Metro Government Network. If External Party does not have a system that is compatible, it is External Party's responsibility to obtain a compatible system.

2.2 External Party shall implement security controls to protect Metro Government Network from risk when its systems or Agents connect to the Metro Government Network. Such controls include, but are not limited to:

2.2.1 Installing and maintaining ICSA Labs certified Anti-virus Software on External Party system and, to the extent possible, use real time protection features. External Party shall maintain the Anti-virus Software in accordance with the Anti-virus Software External Party's recommended practices.

2.2.2 External Party may not access the Metro Government Network with systems that may allow bridging of the Metro Government Network to a non-Metro Government network.

2.2.3 External Party shall only access the Metro Government Network with systems that have the most current Security Patches installed.

3 Use of Remote Support Tools on Metro Government Network.

3.1 External Party shall connect to the Metro Government Network using only Metro Government provided or approved Remote Access Software.

3.2 External Party shall not install or implement any form of permanent Remote Access (e.g., GotoMyPC) on the Metro Government Network or Metro Government systems.

4 Remote Control Software

4.1 External Party may not install any form of Remote Control Software on systems that are maintained or administered by Metro Government without Metro Government's consent. External Party is only allowed to install Remote Control Software on External Party Managed Systems.

4.2 Remote Control Software must secure all network traffic using Strong Encryption.

4.3 External Party shall ensure that Remote Control Software contained within the Product supports the logging of session establishment, termination, and failed login attempts. Each log entry must include the following information about the logged event: date and time of event; type of event; event description; user associated with event; and network identifiers (IP address, MAC Address, etc.) or logical identifiers (System name, port, etc.). For External Party Maintained Systems, External Party shall ensure that such systems are configured to do the above.

4.4 Remote Control Software shall not provide escalation of user account privileges.

4.5 External Party shall only access the Metro Government Network via Metro Government approved remote access methods. External Party shall not supply Products, nor make configuration changes that introduce non-approved forms of Remote Access into the Metro Government Network.

EXHIBIT RM

Risk Management Requirements

1 **Risk Management Practices.** External Party shall implement internal risk management practices to ensure the confidentiality, integrity and availability of Metro Government Information. These practices will be no less secure than the ones used by External Party to protect External Party's own Sensitive Information or information of comparable sensitivity.

2 **Annual Security Assessment.**

2.1 Party shall perform a security assessment of External Party's internal network every year. This assessment shall include an evaluation of risks to the confidentiality, integrity and availability of Metro Government Information which resides on External Party's network or systems and a documented plan to correct or mitigate those risks, as described in industry standard guidance (e.g., NIST Guide for Conducting Risk Assessments, SP 800-30 Rev. 1; currently available at http://csrc.nist.gov/publications/PubsSPs.html) External Party's annual security assessment shall also include an evaluation of External Party's compliance with the terms of this Agreement.

2.2 External Party shall promptly correct any non-compliance with this Agreement. External Party shall report any material non-compliance with this Agreement to Metro Government and shall provide a written plan to correct or mitigate risk identified by External Party's security assessment, if such non-compliance has not been cured, within thirty (30) days following the completion of the security assessment.

3 **Breach Notification.** In addition to the notification requirements in any Business Associate Agreement with Metro Government, External Party shall notify Metro Government of any Data Breach within 24 hours of External Party's actual knowledge or reasonable belief (whichever is earlier) that such breach has occurred ("Breach Notice") by contacting Metro Government ITS Help Desk at (615) 862-HELP and the Information Security Incident contact listed in Exhibit A-3. The Breach Notice should describe the nature of the breach, the scope of the information compromised, the date the breach occurred, and the identities of the individuals affected or potentially affected by the breach as well as specific information about the data compromised so that Metro Government can properly notify those individuals whose information was compromised. External Party shall periodically update the information contained in the Breach Notice to Metro Government and reasonably cooperate with Metro Government in connection with Metro Government's effort to mitigate the damage or harm of such breach.

EXHIBIT SOFT

Software / System Capability

1 Supported Product.

1.1 Unless otherwise expressly agreed by Metro Government in writing, External Party shall provide Metro Government only supported versions of the Product, which will not become “end of life” for at least 24 months. When the Product or Service requires third party components, External Party must provide a Product that is compatible with currently supported third party components. Unless otherwise expressly agreed by Metro Government, External Party represents that all third party components in its Product are currently supported, are not considered "end of life" by the third party provider of such components, and will not become "end of life" in less than 24 months from the date of acquisition by Metro Government.

1.2 If Open Source Software is incorporated into the Product, External Party shall only use widely supported and active Open Source Software in the Product, and shall disclose such software to Metro Government prior to its acquisition of the Product.

2 Software Capabilities Requirements.

2.1 External Party shall disclose to Metro Government all default accounts included in their Product or provide a means for Metro Government to determine all accounts included in the Product.

2.2 External Party shall not include fixed account passwords in the Product that cannot be changed by Metro Government. External Party shall allow for any account to be renamed or disabled by Metro Government.

2.3 External Party's Product shall support a configurable Session Timeout for all users or administrative access to the Product.

2.4 External Party shall ensure that the Product shall transmit and store Authentication Credentials using Strong Encryption.

2.5 External Party Products shall mask or hide the password entered during Interactive User Login.

2.6 External Party shall ensure that Products provided can be configured to require a Strong Password for user authentication.

2.7 External Party’s Product shall allow user accounts to be disabled after a configurable amount of failed login attempts over a configurable amount of time.

2.8 External Party’s Product shall have the capability to require users to change an initial or temporary password on first login.

2.9 External Party’s Product shall have the capability to report to Metro Government, on request, all user accounts and their respective access rights within one (1) business day or less of the request.

2.10 External Party’s Product shall have the capability to function within Metro Governments Information Technology Environment. Specifications of this environment are available upon request.

3 Backdoor Software. External Party shall not provide Products with Backdoor Software, including, without limitation, undocumented or secret access functions (e.g., accounts, authorization levels, over-rides or any backdoor). External Party shall supply all information needed for the Metro Government to manage all access (local or remote) capabilities within the Product including denying of Remote Access entirely from any party including External Party. External Party shall not include any feature within the Product that would allow anyone to circumvent configured authorization remotely.

4 **Remote Access Software.** External Party shall not provide Products that will allow for Remote Access from untrusted networks by default.

EXHIBIT VMGT

External Party Managed System Requirements

1 Vulnerability and Patch Management.

1.1 For all External Party Managed Systems that store Metro Government Information, External Party will promptly address Vulnerabilities though Security Patches. Unless otherwise requested by Metro Government, Security Patches shall be applied within fourteen (14) days from its release for Critical Security Patches, thirty (30) days for Important Security Patches, and twelve (12) months for all other applicable Security Patches. External Party may provide an effective technical mitigation in place of a Security Patch (if no Security Patch is available or if the Security Patch is incompatible) which doesn't materially impact Metro Government's use of the system nor require additional third party products.

1.2 If the application of Security Patches or other technical mitigations could impact the operation of External Party Managed System, External Party agrees to install patches only during Metro Government approved scheduled maintenance hours, or another time period agreed by Metro Government.

1.3 External Party Managed Systems on the Metro Government Network or Metro Government Infrastructure, the Metro Government retains the right to delay patching for whatever reason it deems necessary.

1.4 Metro Government will monitor compliance and check for Vulnerabilities on all Products on the Metro Government Network or Metro Government Infrastructure. External Party shall provide Metro Government administrative credentials upon request for the purpose of monitoring compliance of a given Product. Metro Government will not knowingly change configurations of the External Party Managed Systems without prior approval from External Party.

1.5 Government may monitor compliance of External Party Managed Systems. External Party agrees to allow Metro Government to check for Vulnerabilities during agreed upon times using mutually agreed upon audit methods.

1.6 External Party shall use all reasonable methods to mitigate or remedy a known Vulnerability in the External Party Managed System according to the level of criticality and shall cooperate fully with Metro Government in its effort to mitigate or remedy the same. Upon Metro Government's request, External Party shall implement any reasonable measure recommended by Metro Government in connection with External Party's mitigation effort.

2 System Hardening.

2.1 External Party Managed Systems, External Party shall ensure that either: (i) file shares are configured with access rights which prevent unauthorized access or (ii) External Party shall remove or disable file shares that cannot be configured with access controls set forth in (i) hereof. Access rights to file shares that remain under (i) must use the Principle of Least Privilege for granting access.

2.2 In the event that External Party is providing Products or systems that are to be directly accessible from the Internet, External Party shall disable or allow disabling by Metro Government of all active or executed software components of the Product or system that are not required for proper functionality of the Product or system.

2.3 External Party shall ensure that External Party Managed Systems are synchronized with reliable time sources and have the proper time zone set or no time offset (e.g., GMT or UTC). In the case of systems residing on the Metro Government Network, External Party shall ensure that all such systems are synchronized with an Metro Government corporate timeserver in their respective Regional Data Centers (RDC).

2.4 For External Party Managed Systems, External Party shall remove or disable any default or guest user accounts. Default accounts that cannot be removed or disabled must have their default password changed to a Strong Password that is unique to the respective site and Metro Government.

2.5 For External Party Managed Systems, External Party shall ensure that the system is configured to disable user accounts after a certain number of failed login attempts have occurred in a period of time less than thirty (30) minutes of the last login attempt or that system monitoring and notification is configured to alert system administrators to successive failed login attempts for the same user account.

3 **Authentication**.

3.1 External Party shall assign a unique user ID to any Agent or end user who accesses Sensitive Information on External Party Managed Systems. This unique ID shall be configured so that it enables tracking of each user's activity within the system.

3.2 External Party agrees to require authentication for access to Sensitive Information on External Party Managed System.

3.3 External Party agrees to configure the system to support Strong Authentication for accessing Sensitive Information from any Open Network (e.g., Internet, open wireless). For avoidance of doubt, Metro Government Network is considered a trusted network.

3.4 External Party shall configure the system to expire passwords at least every one-hundred and eighty (180) days and require a password change on the next successful login. For system that cannot support Strong Passwords, External Party shall configure the system to expire passwords every ninety (90) days.

3.5 Unless otherwise agreed by Metro Government, External Party shall ensure that External Party Managed Systems will require Strong Password for user authentication.

4 **Automatic Log off.** External Party shall configure systems which store Sensitive Information to automatically logoff user sessions at the most after 20 minutes of inactivity.

5 **User Accountability.** External Party shall report to Metro Government, on request, all user accounts and their respective access rights within the system within five (5) business days or less of the request.

6 **Data Segregation, Data Protection and Authorization.** External Party shall implement processes and/or controls to prevent the accidental disclosure of Metro Government Sensitive Information to other External Party Metro Governments, including an Affiliates of Metro Government.

7 **Account Termination**. External Party shall disable user accounts of Agents or Metro Government end users for the system within five (5) business days of becoming aware of the termination of such individual. In the cases of cause for termination, External Party will disable such user accounts as soon as administratively possible.

8 **System / Data Access.**

8.1 External Party and its Agents shall only access system, application or data which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent External Party or its Agent from accessing those data or functions outside of Metro Government's authorization. External Party shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.

8.2 External Party agrees to use the Principle of Least Privilege when granting access to External Party Managed Systems or Metro Government Information.

9 **System Maintenance.**

9.1 External Party shall maintain system(s) that generate, store, transmit or process Metro Government Sensitive Information according to manufacturer recommendations. External Party shall ensure that only those personnel certified to repair such systems are allowed to provide maintenance services.

9.2 External Party shall keep records of all preventative and corrective maintenance on systems that generate, store, transmit or process Metro Government Sensitive Information. Such records shall include the specific maintenance performed, date of maintenance, systems that the maintenance was performed on including identifiers (e.g., DNS name, IP address) and results of the maintenance. Upon request by Metro Government, External Party shall supply such record within thirty (30) days.

Exhibit BAA

HIPAA Business Associate Agreement

This Agreement is entered into this _______ day of _________________, by and between **THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY (METRO)**, a metropolitan form government organized and existing under the laws and constitution of the State of Tennessee ("**Metro**" or "**Covered entity**") and **________________________________** ("**Business Associate**").

SECTION 1 - DEFINITIONS

a. **Business Associate**. "Business Associate" shall generally have the same meaning as the term "Business Associate" in 45 CFR § 160.103, and in reference to the party to this agreement, shall mean [***Insert Name of Business Associate***].

b. **Covered Entity.** "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR § 160.103, and in reference to the party to this agreement, shall mean **Metro**. which must fall under one of the following categories:

(1) A health plan.

(2) A health care clearinghouse.

(3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

c. **Disclosure.** "Disclosure" means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

d. **Electronic Media.** "Electronic Media" shall have the same meaning as set forth in 45 CFR § 160.103.

e. **Employer. "Employer" is defined as it is in 26 U.S.C. § 3401(d).**

f. **Genetic Information.** "Genetic Information" shall have the same meaning as set forth in 45 CFR § 160.103.

g. **HITECH Standards**. "HITECH Standards" means the privacy, security and security Breach notification provisions under the Health Information Technology for Economic and Clinical Health (HITECH) Act, Final Rule of 2013, and any regulations promulgated thereunder.

h. **Individual.** "Individual" shall have the same meaning as set forth in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

i. **Person.** "Person" means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.

j. **Privacy Rule.** "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

k. **Protected Health Information.** "Protected Health Information" or "PHI":

(1) Shall have the same meaning as set forth in 45 CFR § 160.103.

(2) Includes, as set forth in 45 CFR § 160.103, any information, *now also* *including genetic information*, whether oral or recorded in any form or medium, that:

(i) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(ii) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

l. **Required By Law.** "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

m. **Secretary.** "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

n. **Security Rule**. "Security Rule" shall mean the Standards for Security of Individually Identifiable Health Information at 45 CFR part 160 and subparts A and C of part 164.

o. **Subcontractor. "Subcontractor" means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.**

p. **Transaction. "Transaction" shall have the same meaning as set forth in 45 CFR § 160.103.**

q. **Catch-all definition.** Terms used but not otherwise defined in this Agreement shall have the same meaning as the meaning ascribed to those terms in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology Act of 2009, as incorporated in the American Recovery and Reinvestment Act of 2009 ("HITECH Act"), implementing regulations at 45 Code of Federal Regulations Parts 160-164 and any other current and future regulations promulgated under HIPAA or the HITECH Act.

SECTION 2 - OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

a. **Permitted Uses of Protected Health Information**. Business Associate shall not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required by Law. Business Associate may: 1) use and disclose PHI to perform its obligations under its contract with Metro; (2) use PHI for the proper management and administration of Business Associate; and (3) disclose PHI for the proper management and administration of Business Associate, if such disclosure is required by law or if Business Associate obtains reasonable assurances from the recipient that the recipient will keep the PHI confidential, use or further disclose the PHI only as required by law or for the purpose for which it was disclosed to the recipient, and notify Business Associate immediately of any instances of which it is aware in which the confidentiality of the PHI has been breached.

b. **Safeguards.** Business Associate shall use appropriate administrative, physical and technical safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement. Business Associate shall develop and implement policies and procedures that comply with the Privacy Rule, Security Rule, and the HITECH Act. The Business Associate must obtain satisfactory assurances that subcontractor(s) will appropriately safeguard PHI.

c. **Mitigation.** Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

d. **Notice of Use or Disclosure, Security Incident or Breach.** Business Associate shall notify Metro of any use or disclosure of PHI by Business Associate not permitted by this Agreement, any Security Incident (as defined in 45 C.F.R. section 164.304) involving Electronic PHI, and any Breach of Protected Health Information within five (5) business days.

(i) Business Associate shall provide the following information to Metro within ten (10) business days of discovery of a Breach except when despite all reasonable efforts by Business Associate to obtain the information required, circumstances beyond the control of the Business Associate necessitate additional time. Under such circumstances, Business Associate shall provide to Metro the following information as soon as possible and without unreasonable delay, but in no event later than thirty (30) calendar days from the date of discovery of a Breach:

(1) The date of the Breach;

(2) The date of the discovery of the Breach;

(3) A description of the types of PHI that were involved;

(4) identification of each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed; and

(5) Any other details necessary to complete an assessment of the risk of harm to the Individual.

(ii) Business Associate shall cooperate with Metro in investigating the breach and in meeting Metro's notification obligations under the HITECH Act and any other security breach notification laws.

(iii) Business Associate agrees to pay actual costs for notification and any associated mitigation costs incurred by Metro, such as credit monitoring, if Metro determines that the Breach is significant enough to warrant such measures.

(iv) Business Associate agrees to establish procedures to investigate the Breach, mitigate losses, and protect against any future Breaches, and to provide a description of these procedures and the specific findings of the investigation to Metro in the time and manner reasonably requested by Metro.

(v) Business Associate shall report to Metro any successful: (1) unauthorized access, use, disclosure, modification, or destruction of Electronic Protected Health Information; and (2) interference with Business Associate's information systems operations, of which Business Associate becomes aware.

e. **Compliance of Agents.** Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Metro, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

f. **Access**. Business Associate agrees to provide access, at the request of Metro, and in the time and manner designated by Metro, to Protected Health Information in a Designated Record Set, to Metro or, as directed by Metro, to an Individual, so that Metro may meet its access obligations under 45 CFR § 164.524, HIPAA and the HITECH Act.

g. **Amendments**. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that Metro directs or agrees at the request of Metro or an Individual, and in the time and manner designated by Metro, so that Metro may meet its amendment obligations under 45 CFR § 164.526, HIPAA and the HITECH Act.

h. **Disclosure of Practices, Books, and Records**. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Metro available to Metro, or at the request of Metro to the Secretary, in a time and manner designated by Metro or the Secretary, for purposes of determining Metro's compliance with the HIPAA Privacy Regulations.

i. **Accounting**. Business Associate shall provide documentation regarding any disclosures by Business Associate that would have to be included in an accounting of disclosures to an Individual under 45 CFR § 164.528 (including without limitation a disclosure permitted under 45 CFR § 164.512) and under the HITECH Act. Business Associate shall make the disclosure Information available to Metro within thirty (30) days of Metro's request for such disclosure Information to comply with an individual's request for disclosure accounting. If Business Associate is contacted directly by an individual based on information provided to the individual by Metro and as required by HIPAA, the HITECH Act or any accompanying regulations, Business Associate shall make such disclosure Information available directly to the individual.

j. **Security of Electronic Protected Health Information.** Business Associate agrees to: (1) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of Metro; (2) ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; and (3) report to Metro any security incident of which it becomes aware.

k. **Minimum Necessary**. Business Associate agrees to limit its uses and disclosures of, and requests for, PHI: (a) when practical, to the information making up a Limited Data Set; and (b) in all other cases subject to the requirements of 45 CFR 164.502(b), to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.

l. **Compliance with HITECH Standards.** Business Associate shall comply with the HITECH Standards as specified by law.

m. **Compliance with Electronic Transactions and Code Set Standards**: If Business Associate conducts any Standard Transaction for, or on behalf, of Metro, Business Associate shall comply, and shall require any subcontractor or agent conducting such Standard Transaction to comply, with each applicable requirement of Title 45, Part 162 of the Code of Federal Regulations. Business Associate shall not enter into, or permit its subcontractor or agents to enter into, any Agreement in connection with the conduct of Standard Transactions for or on behalf of Metro that:

(i) Changes the definition, Health Information condition, or use of a Health Information element or segment in a Standard;

(ii) Adds any Health Information elements or segments to the maximum defined Health Information Set;

(iii) Uses any code or Health Information elements that are either marked "not used" in the Standard's Implementation Specification(s) or are not in the Standard's Implementation Specifications(s); or

(iv) Changes the meaning or intent of the Standard's Implementations Specification(s).

n. **Indemnity.** Business Associate shall indemnify and hold harmless Metro, its officers, agents and employees from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees, arising out of or in connection with any non-permitted use or disclosure of Protected Health Information or other breach of this Agreement by Business Associate or any subcontractor or agent of the Business Associate.

SECTION 3 - OBLIGATIONS OF METRO

a. Metro shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

b. Metro shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Metro has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

SECTION 4 – TERM, TERMINATION AND RETURN OF PHI

a. **Term**. The Term of this Agreement shall be effective as of **[*Insert date*]** and shall terminate when all of the Protected Health Information provided by Metro to Business Associate, or created or received by Business Associate on behalf of Metro, is destroyed or returned to Metro, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this section.

b. Termination for Cause. Upon Metro's knowledge of a material breach by Business Associate, Metro shall provide an opportunity for Business Associate to cure the breach or end the violation. Metro may terminate this Agreement between Metro and Business Associate if Business Associate does not cure the breach or end the violation within the time specified by Metro. In addition, Metro may immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not feasible.

c. Obligations on Termination.

(i) Except as provided in subsection (ii), upon termination of this Agreement, for any reason, Business Associate shall return or destroy as determined by Metro, all Protected Health Information received from Metro, or created or received by Business Associate on behalf of Metro. This provision shall apply to Protected Health Information that is in the possession of subcontractor or agents of the Business Associate. Business Associate shall retain no copies of the Protected Health Information. Business Associate shall complete such return or destruction as promptly as possible, but no later than sixty (60) days following the termination or other conclusion of this Agreement. Within such sixty (60) day period, Business Associate shall certify on oath in writing to Metro that such return or destruction has been completed.

(ii) In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Metro notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information. If Metro does not agree that return or destruction of Protected Health Information is infeasible, subparagraph (i) shall apply. Business Associate shall complete these obligations as promptly as possible, but no later than sixty (60) days following the termination or other conclusion of this Agreement.

SECTION 5 - MISCELLANEOUS

a. **Regulatory References.** A reference in this Agreement to a section in HIPAA or the HITECH Act means the section as in effect or as amended, and for which compliance is required.

b. **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Metro to comply with the requirements of HIPAA or the HITECH Act and any applicable regulations in regard to such laws.

c. **Survival.** The respective rights and obligations of Business Associate shall survive the termination of this Agreement.

d. **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Metro to comply with HIPAA or the HITECH Act or any applicable regulations in regard to such laws.

SIGNATURE PAGE OF BUSINESS ASSOCIATE AGREEMENT BETWEEN THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY AND ________________________________

THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

APPROVED:

____

Department Head

APPROVED AS TO COMPLIANCE WITH PROCUREMENT CODE:

____

Purchasing Agent

APPROVED AS TO AVAILABILITY OF FUNDS:

____

Director of Finance

APPROVED AS TO PROOF OF INSURANCE:

____

Insurance Manager

APPROVED AS TO FORM AND LEGALITY:

____

Metropolitan Attorney

APPROVED:

____

Mayor Karl F. Dean

FILED IN THE OFFICE OF THE

METROPOLITAN CLERK:

Date: _______________________________

BUSINESS ASSOCIATE

Company/Agency/Organization:

____

BY: ________________________________

Print: _______________________________

Title: _______________________________

Sworn to and subscribed to before me, a Notary Public, this ______day of _____________________ , 20 __ , by ____________________________ , the ___________________________ of the BUSINESS ASSOCIATE and duly authorized to execute this instrument on Business Associate's behalf.

____

Notary Public

My Commission Expires ___________